(2026) Privacy & Security Training: Federal & State Healthcare Privacy Laws

This training is created based on federal and state laws, UCI Health policies and procedures, and provides guidance on preventing various types of privacy and security incidents UCI Health experienced in the prior year.

Introduction

Maintaining Privacy is the Right Thing to Do

We've all probably been there before: **having some sort of medical information we want kept private**.

Maybe it's something deeply personal, something you're just tired of having to talk about, or something that is so embarrassing that you hesitate to mention it even to a doctor.

You want it kept private, and understandably so: **you have a right to that privacy**.

Our patients have the same fundamental right. They place their trust in us. As members of the UCI Health workforce bound by the **UC Statement of Ethical Values and Standards of Ethical Conduct**, federal and state laws, and other policies, we have a moral, ethical, and legal responsibility to safeguard their personal and health information as though it were our own, or that of our loved ones.

Note: depending on browser settings, clicking the link above may open a new tab or window and minimize the UCLC module window.

Introduction

A Single Health Care Component (SHCC) is a group of health care entities that work together to provide health care services. The **University of California** is a **Single Health Care Component (SHCC)** under the **HIPAA Privacy Rule**.

At UCI Health, the UCI Medical Center, clinics, and the UCI College of Health Sciences are part of the SHCC. **This training and our Privacy & Security program applies to all of us - faculty, staff, students, trainees, volunteers, and other workforce members who are a part of the UCI Health community.**

The training is updated annually to reflect changes in federal and/or state laws, changes to our policies and procedures, and to provide guidance on preventing the types of incidents we experience.

All workforce members are responsible for understanding their responsibilities in protecting patient information and the content of this training. In the event you are involved in a privacy or security incident, regulators will request proof of your training.

2

[At Least 50 Northwestern Hospital Employees Fired for Accessing Smollett's Profile, Records: Sources]

Note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window.

In 2019, at least 50 employees were fired from Northwestern Memorial Hospital for accessing the medical profile and records of "Empire" actor Jussie Smollett without authorization.

From the article:

One of those employees – identified simply as Susan to protect her identity – said that with one click of her mouse, she was fired from her job as a surgical nurse last week.

“Simply put, it was just morbid curiosity,” she said. “I went into the charting system and started to search his name.”

“I clicked just once,” Susan said. “I never clicked into his chart."

Intentionally or inappropriately accessing a patient's record is a violation of HIPAA.

Patients always have privacy rights and deserve equal protection of their health care record regardless of the circumstances.

3

The following questions should guide your thinking as you progress through this course.

Check each box below to complete the interactive section.

- [ ] What types of information must be protected?

- [ ] How can I maintain the privacy of protected information and why is it important?
- [ ] What rights do patients have regarding access and use of their medical information?
- [ ] What are my responsibilities for reporting privacy and security incidents?

Privacy Laws and PHI

Privacy Laws

Federal and state privacy laws require that we protect an individual's personal and medical information.

At the end of this section, you will be able to:

- Identify the types of information required to be protected under the federal Health Insurance Portability and Accountability Act (HIPAA).
- Identify the types of information required to be protected under California's Confidentiality Medical Information Act (CMIA).
- Identify if the information you come in contact with at work needs to be protected.

1

Federal Privacy Laws: Health Insurance Portability & Accountability Act (HIPAA)

The **Health Insurance Portability and Accountability Act (HIPAA)** helps patients by making it easier for their health information to be shared among the entities who are involved in their health care.

This increase in information sharing, however, comes with requirements to implement privacy and security safeguards.

HIPAA requires UCI Health to:

1. Protect the privacy of a patient's health information.
2. Describe how patient information can be accessed, used, and/or disclosed.
3. Provide physical and electronic security of Protected Health Information ("PHI")
4. Specify the rights of patients relating to their health information.

We must protect all forms of Protected Health Information including:

Click the front of each card below to flip for examples.

Written	e.g. Documents, Mail, Printed Records

Spoken	e.g. Phone Calls, Conversations
Electronic	e.g. electronic medical record (EMR), Billing, Data on flash drives, Laptops, iPads, Smart Phones, Email, Devices, and other systems containing PHI

State Privacy Laws: Confidentiality of Medical Information Act (CMIA)

Click the tab headings to read more on each section.

CALIFORNIA PRIVACY LAWS | PERSONAL INFORMATION | MEDICAL INFORMATION

California's Confidentiality of Medical Information Act (CMIA) requires UCI Health to:

- Protect individuals' personal and financial information.
- Protect individuals' medical and health information.

CALIFORNIA PRIVACY LAWS | PERSONAL INFORMATION | MEDICAL INFORMATION

Personal information includes:

- Name
- Social Security number (SSN)
- Driver's license number
- California identification number
- Credit or debit card or bank account number

- Email address and password
- Other identifiers

CALIFORNIA PRIVACY LAWS | PERSONAL INFORMATION | MEDICAL INFORMATION

- **Medical Information** is individually identifiable information in the possession of or derived from a provider of a healthcare service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.
- The **California Confidentiality of Medical Information Act (CMIA)** prohibits access, use, or disclosure of "medical information" without prior authorization unless permitted by law.
- **This applies to all patient information at UCI Health.**

Protected Health Information (PHI)

Protected Health Information (PHI) is **individually identifiable health information** created, held, or transmitted by a **covered entity** or its **business associate**, in **any form or media**, whether electronic, paper, or oral.

Click the plus signs below to review each section.

Individually Identifiable Health Information —

Information, including demographic data, that relates to:

1. An individual's past, present, or future physical or mental health or condition,
2. The provision of health care or payment for health care, and
3. Directly identifying the individual, or there is a reasonable basis to believe it could be used to identify the individual.

Elements not identifiable on their own could become identifiable if presented together.

Always err on the side of caution and consult experts.

Covered Entity —

The rules apply to **all** health plans, health care providers, and health care billing companies, as well as any businesses that receive or share health information from these entities.

UCI Health is a covered entity.

Business Associate

A person or entity, other than a UCI Health workforce member, who performs functions or activities on behalf of, or provides certain services to, UCI Health that involve access by the business associate to protected health information.

A Business Associate Agreement (BAA) is required for a Business Associate (BA) to access, create, receive, maintain, store, or transmit PHI.

Any Form or Media

We must protect all forms of Protected Health Information including:

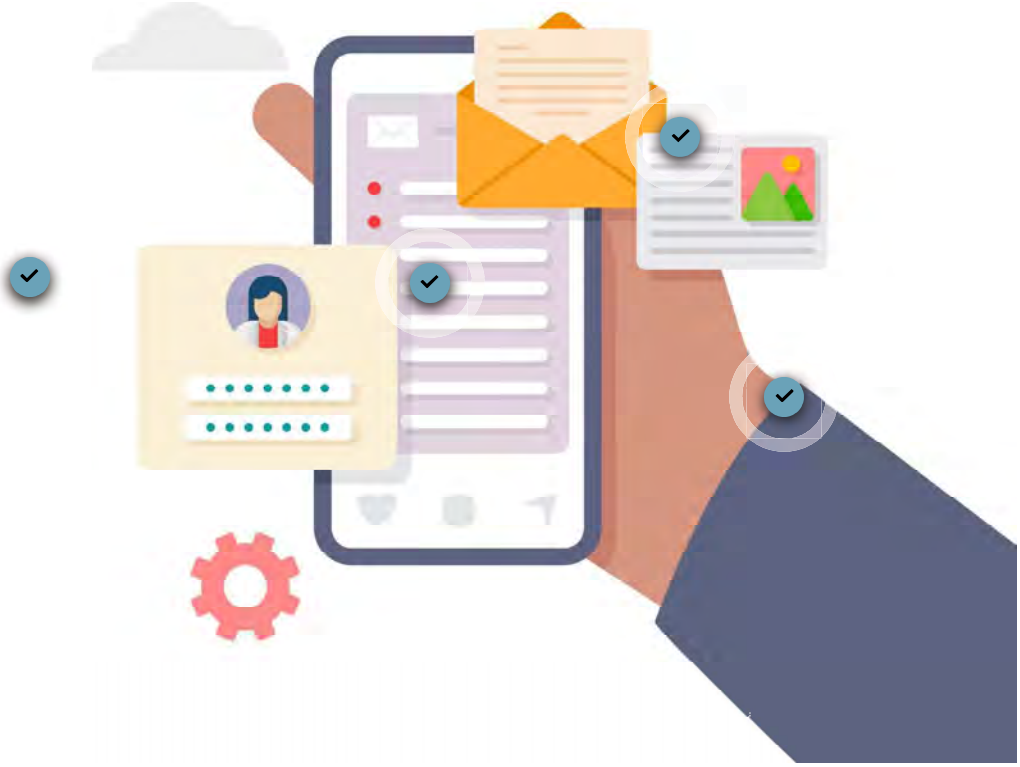
- Written (e.g. Documents, Mail, Printed Records)
- Spoken (e.g. Phone Calls, Conversations)
- Electronic (e.g. electronic medical record (EMR), Billing, Data on flash drives, Laptops, iPads, Smart Phones, Email, Devices, and all other systems containing PHI)

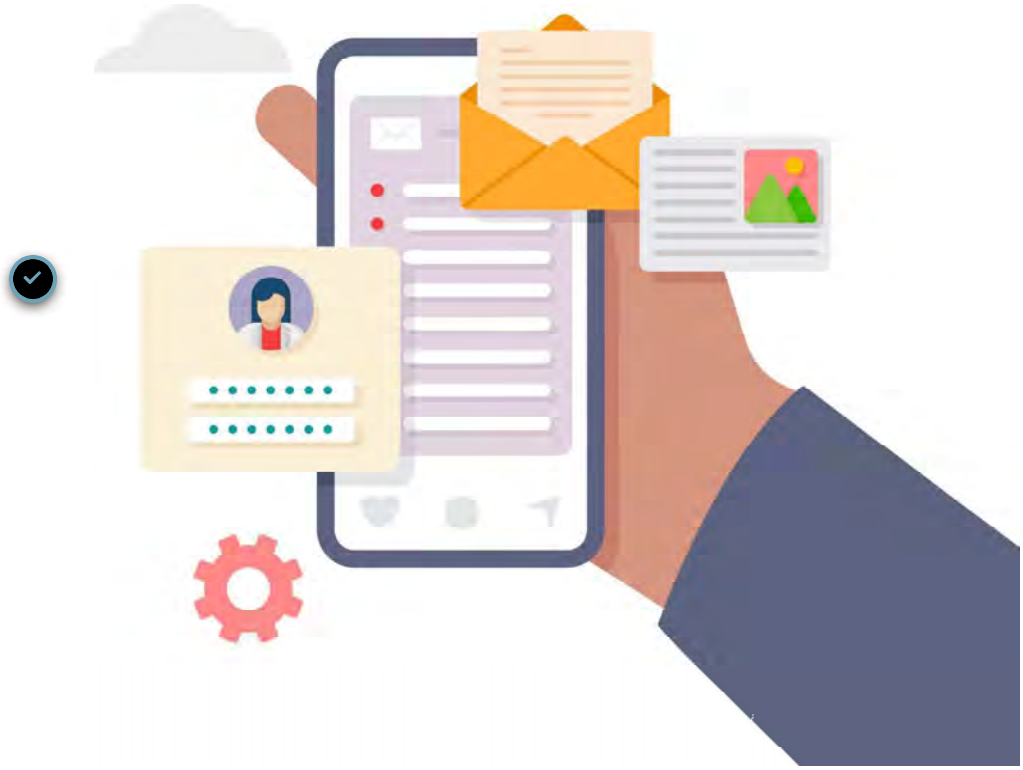
4

Identifiers

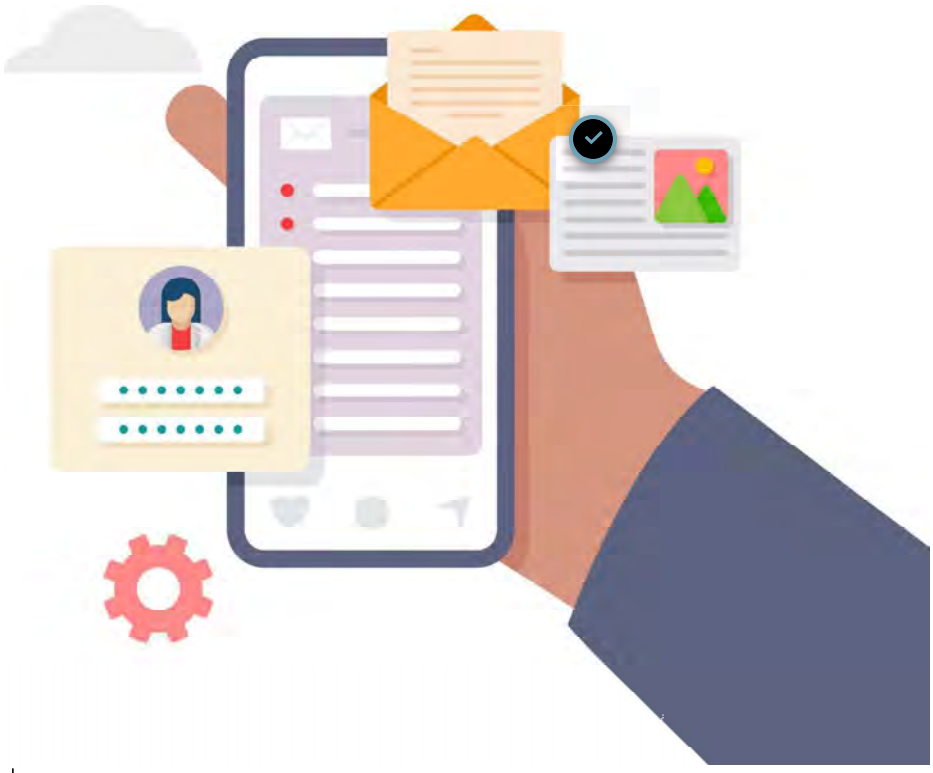
The following identifiers qualify as PHI and must be safeguarded.

Click the first check mark below to review the Identifiers and click the right arrow to continue.





- Name
- Social Security number (SSN)
- Medical record number (MRN)
- Full face photos and other comparable images
- Health plan beneficiary number
- Telephone number
- Fax number
- Email address (with or without password)
- Device identifiers and their serial numbers
- Biometric identifiers (e.g. finger and voice prints)



- Postal address
- URL address
- IP address
- Account numbers
- License/CA ID numbers
- Credit or debit card or bank account number

    - All elements of dates except year
    - Vehicle identifiers and serial number
    - Individually identifiable information regarding a patient's medical history, mental or physical condition, or treatment
    - Individually identifiable health information, including history, lab results, medical bills
    - Any other unique identifying number, code, or characteristic

5

De-identification of PHI

Under certain, limited circumstances, "de-identified" PHI may be disclosed.

De-identification is a complex process, typically involving either a formal determination by specially qualified personnel, or the removal of all the PHI identifiers listed previously.

De-identification is challenging and risky, so consult with your supervisor or the Compliance & Privacy Office before disclosing any possible PHI that you've de-identified.

6

Perspective

There are many different pieces of information we need to protect in the course of our work. Because of this, it can be difficult to remember all of it.

Instead of trying to remember all of the details, take a step back and look at the bigger picture.

Ask yourself, "Does the information I am using help identify a person in some way? Or could it be combined with other information to identify the person?"

If it does, you should treat it as protected information.

If you are not sure, you should STOP and ask your supervisor. Your supervisor can provide direction and support.

7

Summary

You should now be able to:

1. Identify the types of information required to be protected under the federal Health Insurance Portability and Accountability Act (HIPAA).
2. Identify the types of information required to be protected under California's Confidentiality Medical Information Act (CMIA).
3. Identify what information you encounter at work that needs to be protected.

Updates and Lessons from 2025

California Immigration Enforcement

California Senate Bill No. 81 (**review SB-81**), which was recently signed by Governor Newsom on September 22, 2025, brings various changes to California law relating to immigration enforcement at medical centers starting November 4, 2025 (note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window).

Summary of Changes to CMIA
Definitions for “court order” and “search warrant” have been revised.
Required disclosures in response to “court order” and “search warrant” have been revised.

Immigration status (current and prior) or **place of birth** (if known/collected by health care provider) is now considered **“medical information”**.

Healthcare providers are **prohibited** from disclosing **“medical information”** to **immigration enforcement**, unless authorized by the patient or as required/permitted by CMIA.

Best Practices as Recommended by UCOP

1. Inform Risk Management and/or Legal Counsel immediately if Immigration Enforcement requests the following. Check each box below to complete the interactive section.

- [ ] PHI
- [ ] Access to any area
- [ ] Access to a patient

2 Contact Risk Management and/or Legal Counsel immediately if the following is received. Check each box below to complete the interactive section.

- [ ] Subpoena
- [ ] Warrant
- [ ] Court Order
- [ ] Any other requests for review of healthcare provider entity documents.

3 Areas where patients receive care or where PHI is discussed should be non-public. Check each box below to complete the interactive section.

- [ ] Use of appropriate signage, key entry, mapping, or a combination of these is encouraged.
- [ ] Posting of appropriate “notice to authorities” at facility entrances is also encouraged.

4 Staff members should not allow any person access to non-public areas of the facility, unless permitted and/or required by federal or state law. Check the box below to complete the interactive section.

- [ ] If possible, document (including any witnesses) denial for access to non-public areas of facility.

The following UCI Health policies have been updated to reflect the above changes:

- **Review the updated Access, Use, and Disclosure of PHI – Judicial and Administrative Proceedings policy.**
- **Review the updated Disclosures of Protected Health Information to Law Enforcement policy.**

Note: you may need to log in with your HS credentials to access these policies in PolicyStat. Depending on browser settings, clicking the website links may open new tabs or windows and minimize the UCLC module window.

1

Smart Wearable Technology

Smart wearable devices refer to devices that can be worn and include advanced electronic technologies such as photography, audio/video recording, live streaming, and/or AI capabilities.

Examples of smart wearable devices include **Meta Ray-Bans** and **Solos AirGo V2**.

These devices are subject to the same laws, regulations, and policies applicable to other types of electronic/mobile devices.

To ensure regulatory compliance and alignment with UCI Health policies and procedures: Check each box below to complete the interactive section.

- [ ] Only UCI Health ITS-approved technology and devices may be utilized in clinical and secure areas.
- [ ] Smart wearable devices have **not** been approved by UCI Health ITS.
- [ ] Smart wearable devices are **not** permitted in clinical or secure areas.

Employees requiring the use of smart wearable devices (with or without AI capabilities) for accessibility needs in the

workplace should contact Disability Services to initiate a reasonable accommodation request.

UCI Health's **Photography, Filming, and Audio Recording policy** has been updated to reflect the above changes.

Please contact the Compliance and Privacy Office with any questions or concerns.

Note: you may need to log in with your HS credentials to access the above policy in PolicyStat. Depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window.

2

Emergency Contact Use

In 2025, the Compliance and Privacy Office received an unprecedented number of privacy incidents involving clinical staff

members misusing/contacting “emergency contact” on file for non-life-threatening (non-emergent) situations.

Please note that “emergency contact" should only be used when:

1. A patient is unable to communicate or make decisions for themselves (including situations where a patient is unconscious and/or incapacitated).
2. The situation requires immediate action or notification due to a severe (life-threatening) medical emergency.

If a patient has an **advance healthcare directive** (such as power of attorney or will), the document should be followed accordingly, and the emergency contact may be consulted in addition to the designated decision-maker, unless professional judgment deems otherwise.

Examples of Situations

Below are examples of situations when an “emergency contact” may be used. Please note this list is **not** all-inclusive, and providers should **always** use their professional judgment and thoroughly document their actions.

Medical emergencies

When a patient experiences a sudden, severe injury and/or illness.

Incapacitation

When a patient is unconscious, severely confused, or unable to communicate due to a medical condition/injury/illness.

Mental health crisis and/or at risk of harm

When a patient is expressing a mental health crisis and is unable to make decisions or communicate their needs, expressing suicidal thoughts, or is in danger of harming themselves or others.

To obtain consent for treatment

When a patient is unable to consent to a medical procedure due to their condition.

To notify family or loved ones

When a patient needs to be admitted to a hospital or needs to undergo an urgent procedure.

Use and Disclosure of Patient Information

Introduction

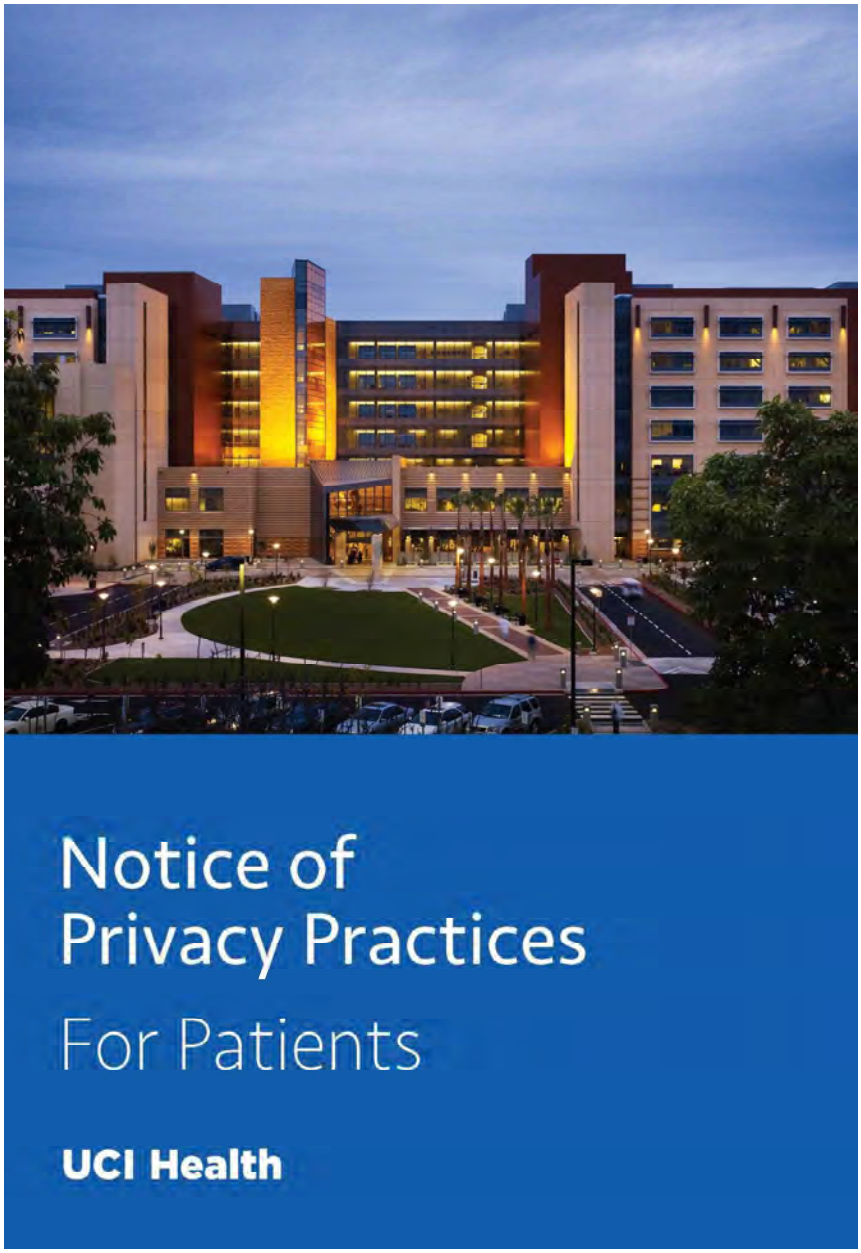
It is important to protect every patient's Protected Health Information (PHI).

At the end of this section, you will be able to:

- Identify guidelines for when you can/cannot access, use, or disclose a patient's PHI.
- Identify specific examples of what you can do to protect patient information.
- Identify guidelines for when it is okay to use/disclose PHI during Patient Treatment, Payment Services, and our internal processes (Healthcare Operations).
- Identify examples of patient privacy rights that patients have to their own health information.

Notice of Privacy Practices

One way that we protect patient information is by giving each patient a Notice of Privacy Practices before collecting, using, storing, or disclosing the patient's PHI.



This notice:

- Describes how UCI Health may use and disclose their PHI
- Advises the patient of their privacy rights

UCI Health must attempt to obtain the patient's signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, UCI Health must document the reason why.

Please carefully **review the Notice of Privacy Practices** so that you are familiar with the notice and what we have told patients about their information (note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window).

The notice must be posted and copies available at all times in all patient registration areas.

Patient Specific Privacy Rights

Patient rights protected under HIPAA and described in the NPP include:

Click the plus signs below to read each right.

Right to Inspect +

The patient has the right to request a copy of their medical record and other health information for inspection.

Right to Amend +

The patient has the right to correct health information that they think is incorrect or incomplete.

Right to Request Confidential Communication +

The patient has the right to request communication in a specific way (for example, home or office phone) or to send mail to a different address.

Right to Request Certain Restrictions +

The patient has the right to request certain health information to not be used or shared for treatment, payment, or operations, so PHI can be kept private and confidential (with permissible use/disclosure exceptions).

Right to Request Accounting Disclosure

The patient has the right to request a list/report (accounting) of who their health information was shared with.

Right to Receive Notice of Privacy Practices

The patient has the right to request a paper copy of the Notice of Privacy Practice at any time.

Right to Choose Someone to Act for You

The patient has the right to give someone the ability to exercise their rights and make choices about their health information (e.g. legal guardian, power of attorney).

Right to File a Complaint

The patient has the right to file a complaint with state or federal regulators.

We must agree to all reasonable requests.

3

Patient Requests for Restriction of PHI

Patients have the right to request a restriction on the use or disclosure of their PHI.

For most restrictions, we are not required to restrict the information if we are unable to comply with the patient's request. NOTE: Please **always** consult with Health Information Management and the Privacy Officer before granting such requests.

However, there is one restriction request we must honor: **If a patient requests to pay in full for a service and asks that we not bill their health insurance, we are required to honor this request.** This also applies if a family member or other individual pays for the service on behalf of the patient.

In this case, we cannot bill the patient's insurance, and we are not permitted to provide the information to the insurance company when submitting information on other services.

Please **refer to the Patient Requests for Restriction of PHI policy** for details on honoring this restriction request including the form patients must complete to request this restriction.

Note: you may need to log in with your HS credentials to access the policy in PolicyStat. Depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window.

4

Prevention of Information Blocking

In 2021, regulations changed to strengthen patients' rights to access and share their electronic PHI. Under the new rules, UCI Health now shares more patient information in MyChart, including most clinical notes and lab results. Notes from all clinical providers documented in electronic medical record (EMR) are shared.

There are very limited exceptions to patients' rights to access and share their PHI, such as:

Check each box below to complete the interactive section.

- [ ] Psychotherapy & Confidential Note Types
- [ ] Staff messages & routing comments
- [ ] Manually blocked information for limited reasons, including preventing physical harm, protecting patient privacy, and legal/administrative infeasibility.

Misuse of these exceptions may place UCI Health at risk of liability under the information blocking regulations. If you have a question on whether it's appropriate to manually block a note, please **consult the Information Blocking policy**, your supervisor, or the Compliance & Privacy Office.

Note: you may need to log in with your HS credentials to access the policy in PolicyStat. Depending on browser settings, clicking the

website link may open a new tab or window and minimize the UCLC module window.

All workforce members should consider the following Best Practices:
Write more "patient friendly" notes by wording them as if you were presenting the information directly to the patient.
Share your screen with the patients when writing the note or read notes out loud to them if possible.
Remove personal contact information, such as your pager number, from the signature line.
Remove any images of your hand-written signature.

5

Patient Requests for Amendment or Addendum of PHI

Due to the new information blocking regulations, patients now have immediate access to more medical information than ever before.

With this increased access, patients may raise questions or concerns with their medical records. Under HIPAA and California privacy laws, patients have a right to request an amendment or addendum to their medical records. UCI Health is not required to honor all patient requests.

Health Information Management (HIM) will not agree to any requests without first speaking to the provider.

All requests for amendments or addendums should be directed to the appropriate UCI Health HIM location.

Orange/Irvine	Fountain Valley	Lakewood	Los Alamitos	Placentia Linda
101 The City Drive S, Bldg. 25A Orange, CA 92868 ROI@hs.uci.edu Phone: 714.456.5670 Fax: 888.522.3679	11170 Warner Ave, Ste 102 Fountain Valley, CA 92708 Phone: 714.966.8024 Fax: 714.966.3398	3700 E South St, Lakewood, CA 90712 Phone: 562.272.6576 Fax: 562.602.6779	3951 Katella Ave. Los Alamitos, CA 90720 Phone: 562.594.3003 Fax: 562.799.3107	1301 N Rose Dr, Placentia, CA 92870 Phone: 714.524.4846 Fax: 714.524.4867

Note: your email may need to be open for the email hyperlink to function properly.

6

Access, Use, and Disclosure of PHI

UCI Health workforce members can access, use, and disclose PHI without the patient's authorization for purposes relating to treatment, payment, and healthcare operations (**TPO**).

Click the tab headings to read more on each section.

TREATMENT | **PAYMENT** | **OPERATIONS**

You may access, use, and disclose medication information about a patient to those involved in the patient's care, such as doctors, nurses, technicians, or providers.

TREATMENT | **PAYMENT** | **OPERATIONS**

You may access, use, and disclose medication information about the patient in order to bill and collect payment for the services the patient received.

TREATMENT | **PAYMENT** | **OPERATIONS**

You may access, use, and disclose medical information for healthcare operation purposes, such as: teaching, medical staff peer review, legal purposes, internal auditing, to conduct customer service surveys, and general business management.

Treatment

Treatment means the provision, coordination, or management of healthcare and related services by one or more healthcare providers, including:

- Coordination or management of healthcare by a healthcare provider with a third party.
- Consultation between healthcare providers relating to a patient.
- Referral of a patient for healthcare from one healthcare provider to another.

Payment

Payment services refers to the activities undertaken by:

1. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan.

2. A healthcare provider or health plan to obtain or provide reimbursement for the provision of healthcare.

These activities relate to the individual to whom healthcare is provided and include, but are not limited to (check each box below to complete the interactive section):

- [ ] Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims.

- [ ] Risk adjusting amounts due based on enrollee health status and demographic characteristics

- [ ] Billing, claims management, collection activities, obtaining payment under a contract for reinsurance

(including stop-loss insurance and excess of loss insurance), and related healthcare data processing.

- [ ] Review of healthcare services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.

- [ ] Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services.

- [ ] Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:
  - Name and address
  - Date of birth
  - SSN
  - Payment history
  - Account number
  - Name and address of the healthcare provider and/or health plan

Operations

Healthcare Operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions.

1. Conducting quality assessment and improvement activities, including:

- Outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities.

- Population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination.

- Contacting of healthcare providers and patients with information about treatment alternatives.

- Related functions that do not include treatment.

2. Reviewing the competence or qualifications of healthcare professionals, evaluating practitioner/provider and health plan performance, conducting training programs in which students, trainees, or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-healthcare professionals, accreditation, certification, licensing, or credentialing activities.

3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for healthcare (including stop-loss insurance and excess of loss insurance). If a health plan receives PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such PHI for any other purpose, except as may be required by law.

4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs.

5. Business planning and development, such as conducting cost-management and planning- related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

6. Business management and general administrative activities of the entity, including, but not limited to:

- Management activities relating to implementation of and compliance with relevant requirements.

- Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policyholder, plan sponsor, or customer.

- Resolution of internal grievances.

- The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will

become a covered entity and due diligence related to such activity.

- Consistent with the applicable requirements of HIPAA, creating identified health information or a limited data set, and fundraising for the benefit of the covered entity.

If you are not sure what constitutes a TPO purpose, you should STOP and ask your supervisor. Your supervisor can provide direction and support.

Accessing Protected Health Information (PHI)

Whenever you access, use, or disclose PHI, there are two overarching rules to which you must adhere.

The first universal privacy rule is the **"need to know" principle**.

Only individuals with a "need to know" should access, use, or disclose patient PHI.

However, this principle does not apply in certain circumstances:

1. If you are disclosing information to a healthcare provider for treatment purposes.
2. If you are disclosing to the patient who is the subject of the information.
3. If you are accessing, using, or disclosing information pursuant to a valid authorization.

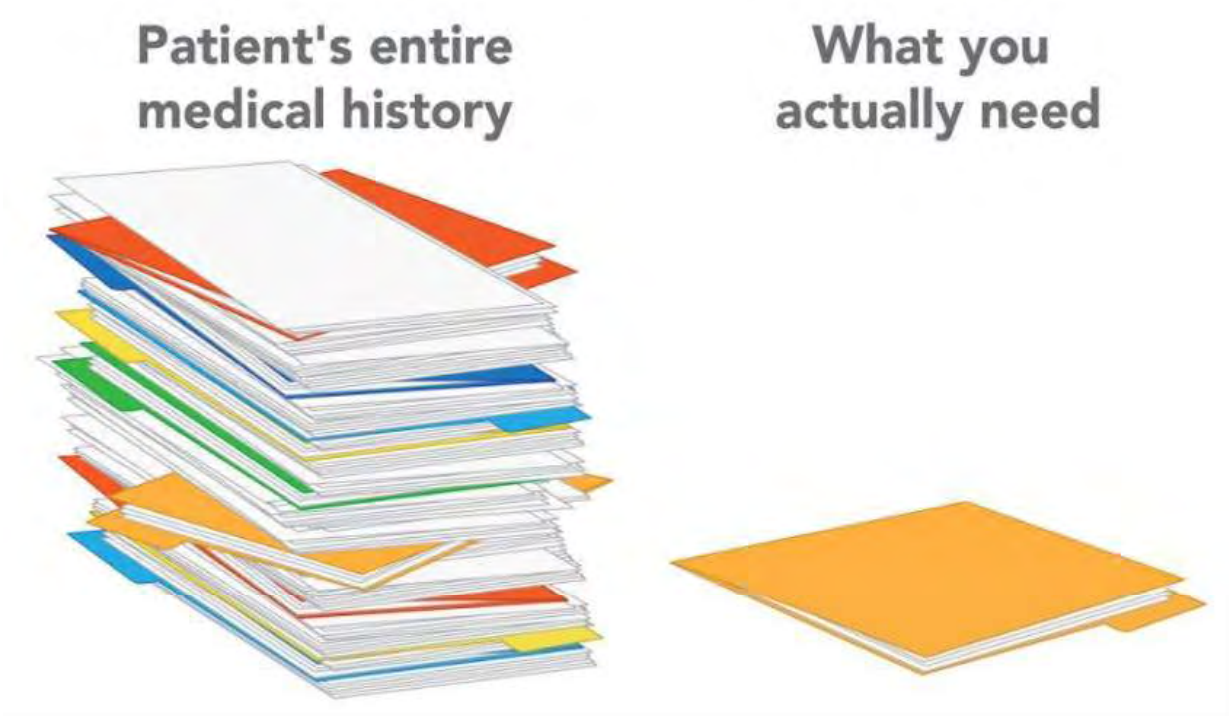
You should only access, use, or disclose PHI that is necessary in order for you to do your job.

If you are unsure whether your access, use, or disclosure of PHI is permitted, ask yourself the following:

- Do I need to access the Protected Health Information to do my job here at UCI?
- How would I feel if someone viewed or discussed my Protected Health Information without authorization?

The second universal privacy rule is the **"minimum necessary" standard**.

The **"minimum necessary" standard** requires that you make reasonable efforts to ensure **only the minimum amount of PHI needed** to **accomplish your intended purpose be accessed, used, or disclosed.** This means that if you are working on a task that can only be accomplished by accessing, using, or disclosing PHI, you must make sure to do so only with the minimum PHI needed to get that job done.



For example: if you're helping an insurer process a payment, and they need the patient's name, date of birth, and an invoice number, you should:

1. Attempt to find the name, date of birth and invoice number in a way that exposes you to as little other PHI as possible, and
2. Make sure you provide the insurer with only the name, date of birth, invoice number **AND NO OTHER PHI**.

Inappropriate Access to PHI

Searching or accessing records belonging to your coworkers, friends, family members, neighbors, or any other patient (including your OWN) without a business or clinical purpose is **strictly prohibited**.

Click the front of each card to flip to review.

DO NOT search or enter records:

Out of curiosity

DO NOT search or enter records:

Due to concern about someone's well-being

DO NOT search or enter records:

To assist someone who is not your patient with obtaining information

Electronic medical record system (EMR) must not be used as a search tool to locate addresses, name spelling, birthdates, or phone numbers. Demographic information that appears when searching an individual is still considered protected health information.

UCI Health workforce members must go through proper channels, such as MyChart or the Health Information Management department, to obtain information about their or their loved ones' healthcare.

Ask your supervisor before accessing or modifying your coworker's record, family member's record, or your own record.

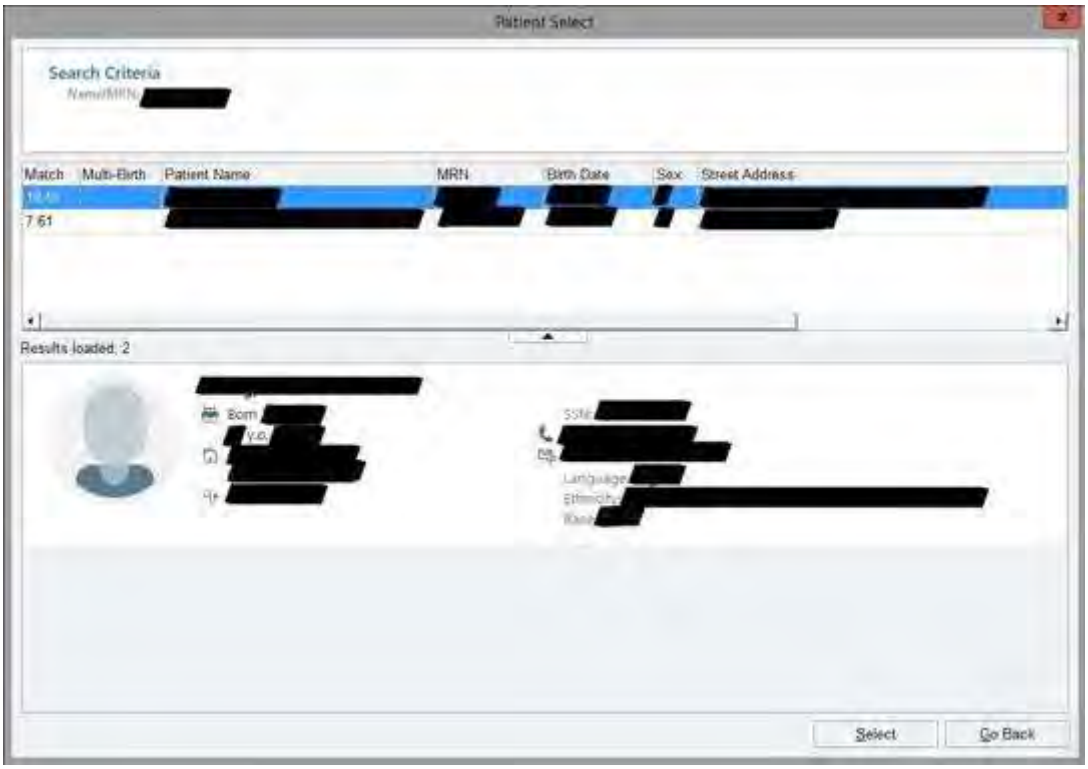
This is only allowed under certain, very limited, circumstances.

2

Patient Identity Reports

Searching for any information in the EMR without a business or clinical purpose is strictly prohibited.

Information contained in the "Identity Report" is PHI – even if you view only the Identity Report, you have violated privacy laws and UCI Health policies if you did not have a business or clinical need to view this information.



3

Attestation

By clicking the I AGREE button below, you attest that you understand the following: Check each box below to complete the

interactive section.

- [ ] You will only access, use, or disclose PHI if it's necessary to perform your job duties. If you don't "need to know" the information to do your job, you will not access, use, or disclose the information.

- [ ] You will only access, use, or disclose the "minimum necessary" information to perform your job. If you're not sure, ask your supervisor for guidance.

- [ ] You will not use EMR without a business or clinical purpose, including searching or accessing medical records belonging to coworkers, friends, family members, and yourself.

- [ ] You will follow UCI Health policies and procedures for information confidentiality.

- [ ] You are responsible for any access, use, or disclosure of UCI Health data that occurs under your UCI Health login credentials, including those in the EMR.

Remember

1. Only access, use, or disclose PHI if it's necessary to perform your job duties. If you don't "need to know" the information to do your job, you shouldn't access, use, or disclose the information.

2. Only access, use, or disclose the "minimum necessary" information to perform your job duties. If you're not sure, ask your supervisor for guidance.

3. Do not use EMR without a business or clinical need, including searching or accessing the medical records of coworkers, friends, family members, and yourself.

4. Follow UCI Health policies and procedures for information confidentiality.

5. Everyone is responsible for any access, use, or disclosure of UCI Health data that occurs under their UCI Health login credentials, including those in the EMR.

Privacy policies can be found on **PolicyStat**, under Policy Area "**Health Enterprise: Privacy & Security**".

Note: you may need to log in with your HS credentials to access the policy in PolicyStat. Depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window.

Lesson 6 of 12

Written Authorization and Communication

When We Need to Get Written Authorization

There are many situations in which we need to get a patient's (or legal representative's) prior written authorization before being able to access, use, or disclose PHI, and there are official UCI Health forms to use in these situations.

Click the first check mark below to read more. Click the right arrow to continue.

For example, we need prior written authorization before disclosing:

- Medical information or records to someone other than the patient
- Information for use in research (clinical trials)
- Patient information for marketing, fundraising, or mass communication (TV, radio, news)

Always use the applicable UCI Health HIPAA authorization form.

Special protections apply to mental health, HIV, substance abuse, and genetic information.

To release this information, the patient must initial the applicable section on the authorization form, otherwise the sensitive information must be withheld or redacted.

If you receive an authorization form from another organization, consult with the Health Information Management department before acting on the authorization.

1

Communication with a Patient's Family and Friends

Unless the patient has prohibited a disclosure, care providers must use professional judgment when determining when and what information to share with family and friends. **Do not reveal past medical problems unrelated to the patient's current condition.**

It is appropriate to share information about a patient with family and friends when:

- The patient implicitly or explicitly consents to the sharing. For example, when a patient asks to bring their spouse or family member in with them to an office visit where their treatment options will be discussed.
- In your best judgment, limited information should be shared to assist with the care of the patient.

For example

Click the plus signs below to read more on each section.

Patient's Mobility Limitations

You can give information about a patient's mobility limitations to a friend driving the patient home from the hospital.

Patient's Payment Options

You can discuss a patient's payment options with their adult daughter.

Patient's Friend

You can instruct a patient's friend, family member, or other caregiver about proper medicine dosage when they come to pick the patient up from the hospital.

Patient's Condition

A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.

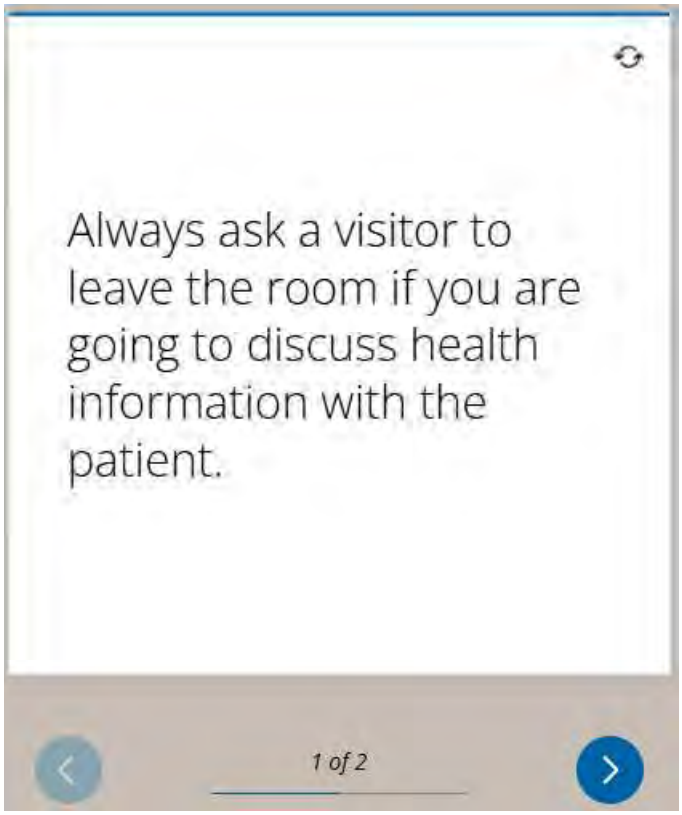
Always be cautious when discussing sensitive information such as HIV/AIDS, STIs, or mental health issues with family members present.

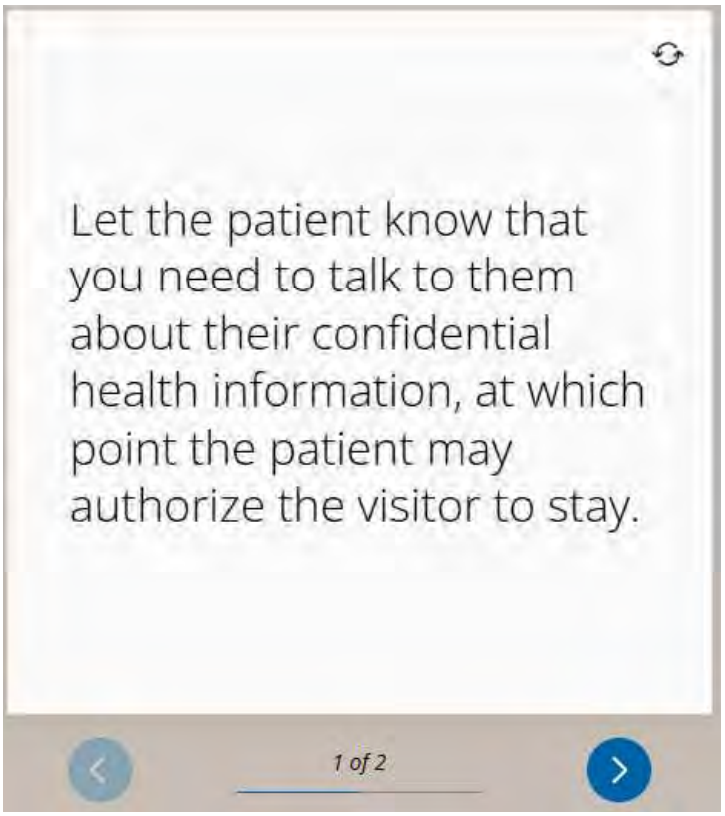
In addition, minor patients in California have the right to confidential reproductive health care, including birth control, abortion, and STI testing. They can consent to these services

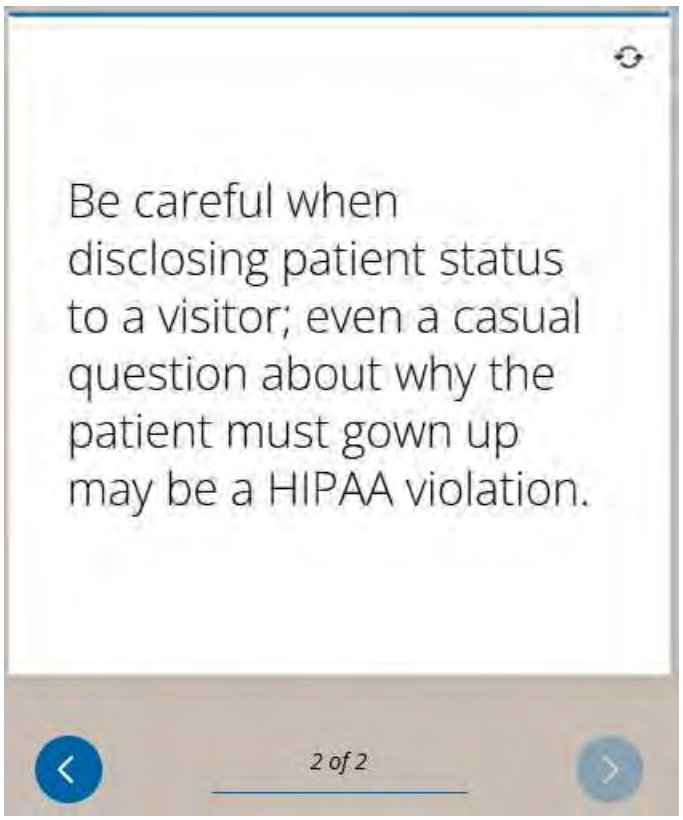
WITHOUT parental permission. **NEVER disclose this information to anyone other than the patient themselves.**

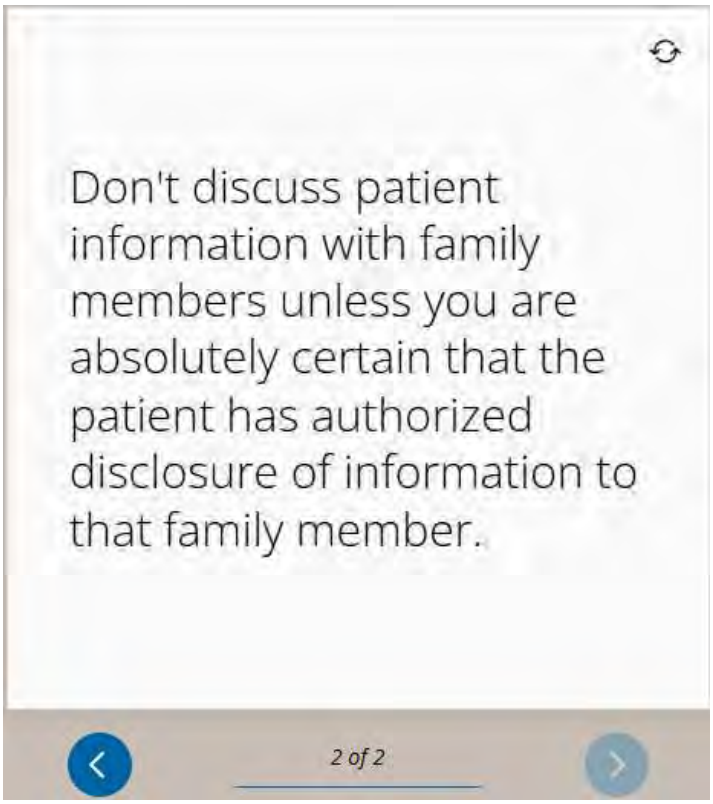
Tips:

Click the front of each card to read more tips and click the arrow to continue.


Always ask a visitor to leave the room if you are going to discuss health information with the patient.
1 of 2


Let the patient know that you need to talk to them about their confidential health information, at which point the patient may authorize the visitor to stay.
1 of 2


Be careful when disclosing patient status to a visitor; even a casual question about why the patient must gown up may be a HIPAA violation.
2 of 2


Don't discuss patient information with family members unless you are absolutely certain that the patient has authorized disclosure of information to that family member.
2 of 2

2

Disclosure by Phone

Facility Census/Directory: Unless a patient has opted-out and does not want to be listed in the directory/census, we can only disclose the location and general health status of a patient to a caller if the caller identifies the patient by name.

- If a caller requests additional information about the patient, do not provide any information unless you are absolutely certain they are authorized individual(s) and/or family/friends **involved** in the care of the patient.
- Contact your supervisor or the Compliance & Privacy Office with any questions or concerns.

3

General Guidelines

Certain departments may have more stringent requirements than what is listed here - contact your supervisor or the Compliance & Privacy Office with any questions or concerns.

Click the tab headings to read each section.

GENERAL CONDITION | CONSENT | OTHERWISE...

Unless opted-out of directory, you may:

- Provide information about general condition **only**.
- If the patient is alert and awake, ask the patient if they want to talk with the caller.
- Refer caller to patient's designated representative for additional details.

GENERAL CONDITION | CONSENT | OTHERWISE...

If the patient is able and consents to take the call, transfer caller to patient.

GENERAL CONDITION	CONSENT	OTHERWISE...
Otherwise, no information can be provided until a written authorization to disclose the information to the caller is obtained from the patient.		

4

Phone Calls: Identity Verification

Remember to inform the caller that we must ask a few questions to verify their identity to protect patient privacy.

When verifying information, **do not provide** any information when asking a question.

For example

Click the front of each card to flip for answers.

Instead of “is your address still 123 Main?”

Ask “what is your address?”

Instead of “are the last four digits of your SSN 1234?”

Ask “what are the last four digits of your SSN?”

If the patient provides information different than what's in our files (EMR)...

Ask them to provide prior information by saying "I have a phone number that starts with 714" or "I show an address in Santa Ana"

Phone Calls: Outpatient Areas

- If a friend or family member of a patient is calling to verify an appointment or obtain information about a specific patient, **before sharing any PHI**:
    - Check any restrictions on disclosures.
    - Ask to speak with the patient, if available, to confirm their consent.
    - Use your best judgment if you know that the caller has been involved with patient care/clinic visits and implied consent by patient.
- **In emergency situations, use your best judgment.**

- If the patient has signed an authorization, verify with caller the patient information that they would be expected to know (e.g. full date of birth, full name, mother's maiden name, last 4 digits of SSN, etc.).
- Only provide the **minimum necessary** amount of information (e.g. only say that patient is ready to be picked up from appointment).

6

Summary

You should now have knowledge of:

1. Examples of patient privacy rights that help protect patients' own health information.
2. Specific examples of what you can do to protect patient information.
3. Guidelines for when you can/cannot use or disclose a patient's Protected Health Information (PHI).
4. Guidelines for using or disclosing PHI during Patient Treatment, Payment Services, and Health Care Operations

Protecting Patient Information

Introduction

In this section of the training, we will outline the various ways that you can protect and secure patient information. We will also cover common types of errors that can occur, which may result in patient information being breached or placed at risk.

While the Information Security (IS) department is responsible for many aspects of information security, **each employee plays a vital role in protecting our patients' information**.

The risks of a breach of patient information include the following:

Click the front of each card to read more and click the arrow to continue.

Electronic Databases

Portable Devices

1 of 3

Emails

Faxes

2 of 3

Hardcopies

Human Error

At the end of this lesson, you will be able to:

- List common types of errors that can result in breach of patient information.
- Identify how to prevent patient information from a breach or unauthorized disclosure.
- Implement best practices to help minimize risks and/or breach of patient information.

1

Electronic Databases

The greatest risk of a data breach is the loss of electronic data or access to computer systems with patient information including, but not limited to, the EMR, Microsoft Office, and SharePoint.

If you are creating such a database, or using a computer program accessible via the internet, please ensure that **Information Technology Services (ITS)** knows about the sensitive information it contains, so that they can ensure it is appropriately protected (note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window).

If you share information about patients with other departments using a SharePoint or a shared network drive, make sure that the permissions on the folders are kept up to date with only those individuals who need the information. Also ensure only the minimum amount of patient information is included in the shared drive.

2

Portable Devices and Media Security

Another risk of a breach comes from databases or files of patient information that are on a portable device.

Examples of such devices include, but are not limited to:

- Laptops
- Desktops
- Mobile phones (“smart phones”)
- USB memory sticks
- CDs
- DVDs
- iPads and other tablets
- Portable Hard Drives

Click the tab headings to read each section.

MEDIA SECURITY | MOBILE DEVICE SECURITY | BEST PRACTICES

Do not store PHI on personal cloud service accounts, such as iCloud or Dropbox. Personal accounts create heightened risk of data breaches. PHI must only be stored on platforms approved by the University to appropriately protect PHI.

Do not use third party messaging or texting applications (such as WhatsApp, Skype, or Viber) with patient information. The version you are using may be sending patient information in clear text for anyone to intercept. Even encrypted versions of messaging applications may not be robust enough and can be intercepted.

Any identifiable patient information inputted or provided to non-approved AI or research technology is a privacy and security violation. Contact the Compliance & Privacy Office to confirm whether a particular tool is approved for use.

Mobile smart phones are often used for email communications. If an email message received on your smart phone includes protected health or other confidential information, this can pose a risk of unauthorized access if the device is lost or stolen since messages can be easily retrieved from the device.

The following are fundamental smart phone practices that will help protect confidential information on the device from unauthorized access:

- In the event the phone becomes lost or stolen, immediately contact the ITS Security Team at **714.456.3333** and request a remote wipe of the phone. Wait to discontinue the service for the phone until after the remote wipe is accomplished. If you discontinue the service on the phone, remote wipe will no longer be available.
- You must enable PIN/password protection on your phone. The more complex the PIN/password, the better. Please contact ITS if you need assistance. (NOTE: Devices using the ITS Exchange system already have this PIN policy applied.)
- Enable the device encryption setting, if available. Please contact ITS if you need assistance.

- Do not store restricted information on the phone's memory card (SD card) or any external storage that has NOT been encrypted.

MEDIA SECURITY | MOBILE DEVICE SECURITY | BEST PRACTICES

- Enroll your device with AirWatch with ITS so that we can remotely wipe your lost or stolen mobile device.
- Turn off Bluetooth, Wi-Fi, NFC, and GPS when not specifically in use.
- Turn on your computer's firewall.
- **Review Mobility Documentation** to see which devices ITS supports and recommends (note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window).
- Never use Facetime, Skype for personal use, or other similar applications with patient information, since the connection may not be secure, and the University does not have a business associate agreement or contract for these services.
- Consult with ITS to set up a secure connection using approved equipment.

PROTECT YOUR PORTABLE DEVICES

Never leave laptops, mobile phones, or tablets unattended or locked in a parked car

Report lost or stolen mobile devices to your supervisor and ITS immediately.

Privacy and Information Security can help mitigate risk to the information.

3

Portable Devices - More Best Practices

- Always use strong passwords, passcodes, and passphrases accordingly. **Review the Password Policy** for additional information.
- Activate a PIN on a mobile device (such as an iPad, mobile phone, etc.) if the device is connected to UCI Health email or if it has any type of PHI on it.
- Do not share credentials (username, password, passcodes, etc.) with anyone.
- Lock or log off portable devices when done.

- Ensure that it is absolutely necessary for business purposes to store patient information on any portable device.

- Only store minimum information necessary to accomplish the business purpose.

- All UCI Health-owned devices must be encrypted. Other portable media should be encrypted where applicable. Please contact ITS for assistance if you're unsure how to encrypt patient information appropriately.

- Physically secure the portable device at all times.

- When disposing of old devices, they must be given to ITS to permanently remove any confidential information prior to disposal.

- Minimize the amount of PHI via text or page even when using ITS-approved methods.

- Do not connect devices for power charging to UCI Health computers. This can introduce viruses into our protected network.

Note: you may need to log in with your HS credentials to access the above policy in PolicyStat. Depending on browser settings, clicking

the website link may open a new tab or window and minimize the UCLC module window.

4

Artificial Intelligence (AI) & Electronic Technology Use

To ensure compliance with UCI Health policies and procedures (check each box below to complete the interactive section):

- [ ] Only UCI Health ITS-approved electronic technology may be used.
- [ ] Only UCI Health devices or ITS-approved personal devices equipped with appropriate safeguards may be used.
- [ ] Only UCI Health ITS-approved AI technology including, but not limited to, ambient-listening/recording devices/tools may be used.
- [ ] **Consent** must be obtained from **all** parties prior to utilizing any AI technology.

- [ ] Providers must **document** consent and any applicable disclaimers for AI usage during usual course of patient care.

5

Best Practices

AI Technology Use

- Do not enter any PHI or patient information into AI applications that have not previously been approved for use.
    - Most common publicly available tools, including OpenAI, ChatGPT, and Open Evidence, are **not** approved for use with UCI Health PHI or other sensitive data
- Programs that advertise themselves as “HIPAA-compliant” must still be approved by UCI Health prior to use with any PHI or other sensitive data.

- Contact your manager to find out about approved tools prior to any use.
- If you discover the use of non-approved AI programs with PHI, report to the Compliance and Privacy Office **immediately**.
- Contact ITS or the Compliance and Privacy Office if you have any questions.

Electronic Meetings, Communications, and Recordings

- Only UCI Health ITS-approved platforms and technology may be used for electronic meetings and communications.
- Only UCI Health ITS-approved secure communication methods can be used for communication related to a patient and/or containing PHI.
- **Consent** must be obtained from **all** parties prior to recording any communication (whether via meeting platform, AI ambient-listening/recording, or any other form of recording).
- Routine recording of meetings is **discouraged** to ensure the comfort and psychological safety of all attendees while promoting healthy dialogues.

- Electronic (virtual) meetings should **never** be recorded when sensitive, confidential, or privileged information is being discussed. Such information includes, but is not limited to, the following (check each box below to complete the interactive section):

☐ PHI

☐ Quality/Patient Safety Incidents

☐ Sensitive/confidential/proprietary business information

☐ Medical Staff Meetings (e.g. Peer Review, department meetings)

☐ Meetings and discussions subject to Attorney-Client Privilege

- Educational or training sessions may be recorded if they do not contain any of the above type(s) of sensitive, confidential, or privileged information.

Associated Risks

Emails

A lot of personal information is often communicated via email, and much of it is routinely kept within email accounts. Remember that including restricted information in your email communication presents a security risk. If an unauthorized person gains access to the email accounts, this personal information is potentially vulnerable.

In order to protect patient information in email accounts, minimize your use of email for communicating confidential and personal information.

- Encourage patients to use Secure Health Messaging and the **MyChart patient portal** when communicating with their healthcare providers.
- Please **review the Email and Use of Patient Confidential Information policy** for more information. A consent form

must be completed and uploaded into the patient's chart prior to communicating PHI to patients via email.

Emails sent within UCI Health's secure network (**hs.uci.edu** email addresses) are always encrypted by default.

In the rare cases where it is a business requirement to send PHI to an external email account (anyone with a non-UCI Health email address including UCI Campus [**uci.edu**]), the information being transmitted **MUST** be sent using **[ucsecure]** encryption, which will be explained below.

Note: you may need to log in with your HS credentials to access the above policy in PolicyStat. Depending on browser settings, clicking the website links may open new tabs or windows and minimize the UCLC module window.

1

Secure Email & DLP

The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

Click the plus signs below to read more on each section.

Data Loss Prevention (DLP) —

UCI Health has implemented Data Loss Prevention (DLP) technology to prevent the unencrypted transmission of PHI from UCI Health email accounts.

Proactive Service —

DLP is a proactive service that scans all email content for PHI.

DLP Technology —

DLP technology blocks any unencrypted email message that it identifies as possibly containing PHI and sensitive/confidential information (i.e. SSN).

Compliance & Privacy Office —

The Compliance & Privacy Office is responsible for monitoring DLP and any unsecured PHI that is leaving the organization, as well as any PHI that is sent securely to an outside entity.

How to send Secure Email:

Use **[ucsecure]** including square brackets in the subject line. It must be within the first 150 characters of the subject line for the secure email gateway to detect it.

Things to remember:

- **DO NOT include PHI in the subject line.** While DLP technology encrypts the email and attachments, it does not encrypt the subject line. This means any PHI included in the subject line is viewable by the recipients.
- **DOUBLE CHECK the recipient's email address before sending.** Be careful with autofill!
- **ALWAYS VERIFY the information being sent.** Sending the wrong information to an intended party is also a potential privacy breach.
- **LIMIT the amount of data being sent.**

- For example, if you are attaching an Excel file with 17 columns of data but the recipient only needs the first 3 columns, we recommend deleting the other 14 columns.
- For more information about Secure Email & DLP, please visit the **ITS website** (note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window).

2

Protecting Patient Information When Using Email

Check each box below to complete the interactive section.

- [ ] **Never** share your password with anyone!
- [ ] Protect the email account by using strong passphrases. **Review the Password Policy** for more information.
- [ ] Verify the email address to whom you are sending the email.

- [ ] If the email containing PHI is being sent outside of the UCI Health secure network, it must be encrypted using **[ucsecure]**.

- [ ] **Do not** send PHI or other information to patients via text message or email unless using department-approved tools and procedures.

- [ ] Communicate only the minimum confidential information or PHI necessary.

- [ ] Emails being sent over the Internet from public locations away from the University should not include restricted information, since these emails are not encrypted.

- [ ] **Resist temptation to open attachments or click on links from an unknown or unverified source. Don’t respond to or forward suspicious emails to coworkers. Immediately notify Information Security by utilizing Proofpoint's "Report Suspicious" tool button in Outlook, or by forwarding suspicious emails to security@hs.uci.edu. Delete the email.**

- [ ] Make sure that you have installed the latest security updates (or "patches") for your operating system and applications.

- [ ] Never deactivate your computer's antivirus or protective software.
- [ ] Make sure that protective software and accompanying definition files are updated frequently and automatically.
- [ ] Configure your antivirus to scan all downloaded files, removable media, and email attachments automatically.
- [ ] Don't click on unknown links in emails, texts, instant messages, social networking sites, ads, or pop-ups.
- [ ] Only download files and plug-ins from trusted sources, and don't use untrusted portable media, such as a stranger's flash drive. Also, don't download plug-ins to view pictures, videos, music and other content online without verifying their legitimacy. These often contain malware.
- [ ] Contact the **ITS Service Desk** at **714.456.3333** if you believe your computer is infected with malware. Disconnect the computer from the network immediately to keep the infection from spreading or sending information to an attacker.
- [ ] Be prudent when browsing the web, opening email attachments, clicking on links, and downloading

shared files.

- [ ] If you believe your user ID and/or password have been compromised, immediately change your password and contact the ITS Service Desk.

- [ ] Do not write down your passwords or post them in your work area (such as Post-Its on screen/drawer).

Note: your email may need to be open for the email hyperlink above to function properly. You may need to log in with your HS credentials to access the above policy in PolicyStat. Depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window.

3

Ransomware

Ransomware is a type of malware (malicious software) that encrypts data with a key known only to the hacker and makes the data inaccessible to authorized users. After the data is encrypted,

the hacker demands that authorized users pay a ransom in order to obtain a key to decrypt the data.

Ransomware frequently infects devices and systems through spam, phishing messages, websites, and email attachments and enters the computer when a user clicks on the malicious link or opens the attachment.

One of the biggest current threats to health information privacy is the serious compromise of the integrity and availability of data caused by malicious cyber-attacks on electronic health information systems, such as through ransomware. **The FBI has reported an increase in ransomware attacks and media have reported a number of ransomware attacks on hospitals.**

The **Security Management Process** standard of the HIPAA Security Rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all of the ePHI the entities create, receive, maintain, or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level.

For additional information, please visit the **ITS website**, or call the Service Desk at **714.456.3333** (note: depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window).

4

Faxes

One of the most commonly reported violation of patient privacy occurs when patient information is either faxed to the wrong fax number or the fax includes information of another patient.

The number of faxes going to the wrong fax number has increased with the use of E-Faxing. **You can help reduce these**

by:

- Verifying with patient the name of their healthcare providers.
- Double checking you have selected the correct provider.
- Asking the patient to verify information on face sheet is correct and initial/sign it before adding it to the patient's chart.
- Notifying HIM if you learn that a provider has new contact information.

To protect patient information when sending faxes:

1. Verify the fax number before pushing the send button.
2. Double check that only the information on the correct patient is included in the information being faxed.

3 When dictating reports, make sure the referring physician is correctly listed (e.g. full name or spelled out).

4 Only use the official UCI Health fax cover sheet.

5

Paper

Another risk to patient privacy occurs when patient information is left unattended in areas that are accessible to non-UCI Health workforce members.

NOTE: Even areas that are designated as “staff only” areas can cause problems if the door to the area is unlocked or unmonitored, and anyone can wander into the area.

To protect patient information left in unattended areas (click the first check mark below to read each and click the right arrow to continue):

- Keep documents and paperwork containing confidential information covered and placed in an appropriately secured area, folder, or cabinet.
- Ensure that when you leave the area unattended, no patient information is left out.
- Dispose of material containing patient health information in a confidential shred container.
- Do not carry any printed patient information out of clinical care areas for convenience (e.g. restroom, cafeteria). If you must carry paper, ensure they remain on your person at all times and are never left unattended.
- Do not prop doors open, making confidential information accessible to anyone walking by.
- If you see someone in an area where patient information is being used, verify that they have a job responsibility to be there by confirming they have an ID badge. If the individual is a vendor, they should be accompanied by a UCI Health workforce member and have a vendor badge with their photo and current date.

6

Human Error

Another common problem occurs when printed paperwork, such as lab requisition orders, After-Visit-Summary (AVS), and discharge instructions, is handed to patients when they are mixed with another patient's paperwork. This can be particularly harmful for the patient if the information includes their diagnosis, treatments, and medications.

Similarly, when mailing information to a patient, always make sure the correct information is placed in the correctly addressed envelope. Always double check before sealing the envelope.

To protect patient information when discharging patients (click the first check mark below to read each and click the right arrow to continue):

- Double check that you have the correct patient and the correct information.
- Ensure that you've correctly registered the patient under the correct Medical record number (MRN).
- Ensure that you've correctly entered the information into the correct record.
- Confirm that you have printed out the correct record.
- Confirm that the correct patient's information is on **each page**.

7

Photography

Check each box below to complete the interactive section.

- [ ] PHI includes any photograph of a patient that is identifiable. It is often impossible to de-identify the image of a patient's face or other unique features such as a tattoo or scar.

- [ ] If the photo is being used for patient care, the photo must be included in the patient's medical record. No authorization is required.

- [ ] If the photo is being used for any other purpose, such as teaching or research, an appropriate authorization must be obtained.

- [ ] Refer to the Photography, Filming, and Audio Recording Policy for more information.

- [ ] The authorization forms are on the Compliance & Privacy website.

- [ ] If the image is being used for teaching or research purposes, the image must be downloaded to a secure encrypted server as quickly as possible.

- [ ] The images must then be deleted from the camera or recording device after download, or if the image is no longer needed.

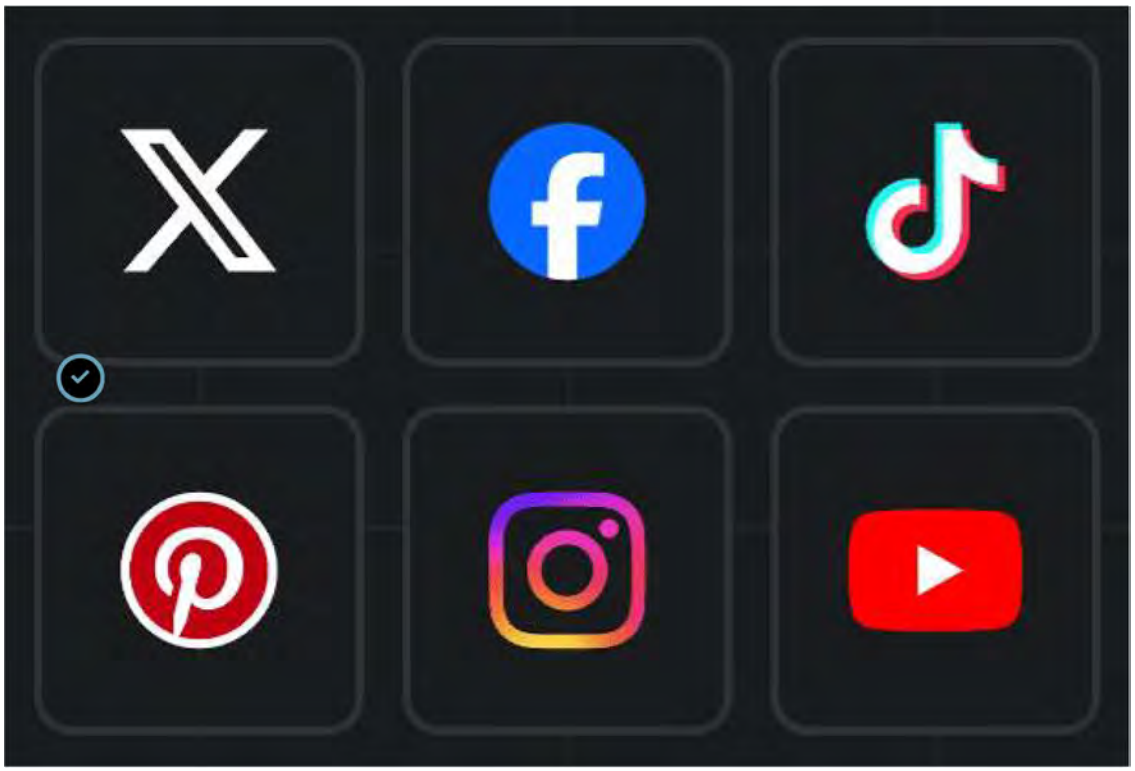
- [ ] The images must not be uploaded to a third-party cloud computing site unless the Chief Information Security Officer has approved the third-party cloud computing.

- [ ] Patients and their families may only record staff and providers with express permission.

Note: you may need to log in with your HS credentials to access the above policy in PolicyStat. Depending on browser settings, clicking the website links may open new tabs or windows and minimize the UCLC module window.

Social Media

Click the first check mark below to read more. Click the right arrow to continue.



- Social media poses significant risks to patient privacy.
- Staff working in healthcare often want to relieve stress of job by sharing
- information with others.
- Risks are present even when patients are not identified by name. Enough circumstantial information can be provided that others will be able to identify the patient.
- **NO** patient information should ever be posted to social media sites, regardless of whether it includes the patient's name or identity.
- Posting photos (even if they are deidentified) is prohibited.

Privacy

Never post Protected Health Information (PHI) - **no** exceptions.

Responsiveness

Monitor your web page and respond to questions and concerns. When appropriate, respond offline.

Reporting

Contact the Compliance & Privacy Office if you have concerns about what you have viewed on social media.

Respect

You are a member of the UCI Health community. Be mindful of the information you post on social media.

Social Media Policy

Please **review the Social Media Policy** for more information. Contact the Compliance & Privacy Office for any questions or concerns.

Note: you may need to log in with your HS credentials to access the policy in PolicyStat. Depending on browser settings, clicking the website link may open a new tab or window and minimize the UCLC module window.

9

Social Engineering

Social engineering is the process of obtaining information by manipulating and exploiting the goodwill of others.

The “social engineer” typically calls or sends an email pretending to be someone else or shows up at your workplace under false pretext. Social engineers are interested in gaining access to organizational and personal information, primarily to perpetuate fraud, commit industrial espionage, or simply to disrupt activities.

A social engineer is on the lookout for bits of information that can help them assume someone else's identity, usually without that person's knowledge.

The information they want includes:

Click the front of each card to read more.

Passwords

Personal information

Bank account and credit card information

Sensitive business information

Social Engineering section – missing verbiage of 3rd flip card

The following best practices will help ensure better protection for your personal information and the University's sensitive and confidential information.

Click the tab headings to read more on each section.

DON'T GIVE... | BE CAUTIOUS... | YOUR PASSWORDS...

Don't give private information to anyone you don't know or who doesn't have a legitimate need for it (whether in person, over the phone, via email or the Internet).

DON'T GIVE... | BE CAUTIOUS... | YOUR PASSWORDS...

Be cautious about what you say in elevators, restaurants, trains, buses, and other public places.

DON'T GIVE... | BE CAUTIOUS... | YOUR PASSWORDS...

Your passwords belong to you. **Never** disclose them to anyone.

SHRED... | IF AN UNKNOWN PARTY... | REPORT...

Shred sensitive and confidential information in a confidential shred container. **Never** put it in the garbage intact.

SHRED... | IF AN UNKNOWN PARTY... | REPORT...

If an unknown party is present in your office, request identification and escort the stranger to their host. If they do not know the location of their host, direct them to the Security Office or front desk reception area.

SHRED... | IF AN UNKNOWN PARTY... | REPORT...

Report suspicious behavior and calls to your supervisor.

Complete the interactive content above to continue with the lesson.

Summary

You should now have knowledge of:

1. Ways to prevent a data breach or unauthorized disclosure of patient information.

2. Specific examples of what you can do to protect patient information.

Privacy & Security

Importance of Privacy & Security

It is important for employees to maintain the privacy and security of patient information and understand your responsibilities.

At the end of this section, you will be able to:

- Know how and when to report violations in privacy and security or unauthorized disclosure of patient information.
- Identify the importance of maintaining the privacy and security of patient information.

1

Reporting a Privacy or Security Violation

To report a privacy or security violation:

Click the plus signs below to read each section.

Notify

Notify your supervisor or manager immediately.

Complete Incident Report

Complete an online incident report on the Safety & Quality Information System (SQIS) located on the UCI Health Intranet: Incident Report.

Contact

Immediately contact the Compliance & Privacy Office at **888.456.7006** or **hacompliance@hs.uci.edu** (note: your email may need to be open for the email hyperlink to function properly).

Electronic Information

If it involves electronic information, please also contact ITS at **714.456.3333**.

Theft

If there has been loss/theft of a computer/laptop/electronic device, please immediately notify ITS at **714.456.3333** and/or the UCI (or local) Police Department.

2

Everyone at UCI is responsible for identifying and reporting suspected or known privacy incidents as soon as you become aware.

3

Privacy Violations

Privacy Violations can result in Fines & Penalties

- HIPAA and California's information privacy laws impose significant fines for breaches or other misuses of patient information.
- Fines depend on whether the breach could have been avoided and whether the organization acted quickly to correct the breach.
- This is why we rely on each workforce member to take immediate action when they know of or suspect a breach!

Lesson 9: Privacy & Security

Privacy Violations section – missing flip card verbiage

4

Potential Federal Fines & Penalties

As of 1/28/2026:

VIOLATION CATEGORY	PENALTY RANGE FOR	MAXIMUM PENALTY FOR ALL

	EACH VIOLATION	VIOLATIONS OF AN IDENTICAL PROVISION IN A CALENDAR YEAR
Did not know (and by exercising reasonable diligence, would not have known) that it violated the applicable provision.	$145 to $73,011	$2,190,294
Violation is due to reasonable cause and not to willful neglect.	$1,461 to $73,011	$2,190,294
Violation is due to willful neglect and was corrected during the 30 day period beginning on first day entity	$14,602 to $73,011	$2,190,294

knew (or should have known).		
Violation is due to willful neglect and was not corrected during the 30 day period beginning on first day entity knew (or should have known).	$73,011 to $2,190,294	$2,190,294

Resources

Information Security:

- Your supervisor/manager
- Your department's IT staff
- ITS Service Desk: **714.456.3333**

- Chief Information Security Officer: **Shawn Kelly**

Privacy and Confidentiality:

- Your supervisor/manager
- Compliance & Privacy Office
  Email: **hacompliance@hs.uci.edu**
- Compliance & Privacy Office Phone: **714.456.7006** (Internal: **120.7006**)
- Confidential Compliance Reporting Hotline: **888.456.7006**
- **UCI Health Privacy Compliance website**
- **UCOP Privacy Compliance website**

Policies and Procedures are available on **PolicyStat**.

Note: your email may need to be open for the email hyperlinks above to function properly. You may need to log in with your HS credentials to access PolicyStat. Depending on browser settings, clicking the website links may open new tabs or windows and minimize the UCLC module window.

Confidentiality Agreement

In order to receive credit for completing this course, you will need to read and agree to the following Confidentiality Agreement:

The protection of health and other confidential information is a right protected by law and enforced by individual and institutional fines, criminal penalties, and UC and UCI Health policies and procedures. Safeguarding confidential information is a fundamental obligation for all UCI Health workforce members including employees, faculty, staff, volunteers, students/trainees, contractors, consultants, and vendors doing business with UCI Health, including any individuals affiliated with third parties that access UCI Health systems and data.

I understand and acknowledge that (check each box below to complete the interactive section)**:**

- [ ] I will always protect the privacy and security of confidential information, both during and after my employment with the University of California has terminated.

- [ ] I agree to (a) access, use, or view confidential information to the minimum extent necessary for my assigned duties; and (b) disclose such information only to persons authorized to receive it.

- [ ] I understand that UCI Health may conduct surveillance of all users' access to electronic records to monitor, detect, and identify suspicious and/or inappropriate access of patient and employee records.

- [ ] I understand that any identifiable patient information inputted or provided to non-approved AI or research technology is a privacy and security violation. I will contact the Compliance & Privacy Office to confirm whether a particular tool is approved for use.

- [ ] Inappropriate access, use, or disclosure of protected information will result in disciplinary action, up to and including termination of employment, and may result in a report to authorities charged with professional licensing, enforcement of privacy laws, and prosecution of criminal acts. The State of California may levy penalties to individuals or

providers of healthcare up to $250,000 per violation, depending on the circumstances.

- [ ] User credentials must not be shared. Inappropriate use of my credentials (whether by me or anyone else) is my responsibility and exposes me to severe consequences.

- [ ] I must adhere to all University Privacy and Information Security policies.

- [ ] The Compliance & Privacy Office is available to answer any and all questions and concerns I may have regarding patient privacy. The Compliance & Privacy Office can be reached at **714.456.7006** or **hacompliance@hs.uci.edu** (note: your email may need to be open for the email hyperlink to function properly).

By clicking **I AGREE** below, I attest that I have read and understand the UCI Health Privacy & Security Training and the Confidentiality Agreement. Furthermore, I agree to abide by University of California policies, UCI Health policies, and federal/state privacy laws.

UCI Health

Acknowledgement of Review of the UCI Health Privacy & Security Training: Federal & State Healthcare Privacy Laws

By signing below, I acknowledge that I have read the University of California Privacy Training course and confidentiality statement and agree to abide by UC policy and Federal/State privacy laws.

_____	_____
Student Name	Student Signature
_____	_____
Date	School

_____

School Coordinator Date

Please note that only this page from this packet needs to be returned to the Education Department.